



**Carnegie Mellon  
Software Engineering Institute**

---

Pittsburgh, PA 15213-3890

# Advanced Risk Analysis for High-Performing Organizations

Christopher Alberts  
Audrey Dorofee

Sponsored by the U.S. Department of Defense  
© 2006 by Carnegie Mellon University

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE <b>2006</b>		2. REPORT TYPE		3. DATES COVERED <b>00-00-2006 to 00-00-2006</b>	
4. TITLE AND SUBTITLE <b>Advanced Risk Analysis for High-Performing Organizations</b>				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>Carnegie Mellon University, Software Engineering Institute, 5000 Forbes Avenue, Pittsburgh, PA, 15213-3890</b>				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release; distribution unlimited</b>					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT <b>Same as Report (SAR)</b>	18. NUMBER OF PAGES <b>37</b>	19a. NAME OF RESPONSIBLE PERSON
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>			



# Changing Operational Environment

## From

Centralized management  
control of processes

Dedicated, stand-alone  
technologies

Permanent enterprise, defined  
by organizational chart

One team, one mission

Compartmentalized view of risk  
(e.g., project, security)

## To

Distributed management  
control of processes

Interoperable, networked  
technologies

Virtual enterprise, defined by  
mission

Many teams, one mission

Integrated view of risk



# Changing Risk Profiles

Changes in operational environments are driving the need for advanced risk analysis techniques.

- The operational environment is becoming more complex (e.g., distributed processes).
- New types of risks have emerged from this complexity.
  - inherited risk
  - new sources of risk (e.g., cyber-security risks)
  - risk from combinatorial effects
  - risk from cascading consequences
  - risk from emergent threats



## **The Need for Advanced Techniques**

High-performing organizations are able to manage traditional risks.

Risks arising from operational complexity are often subtle in nature, but bring the potential for catastrophic consequences.

High-performing organizations have the basic skills needed to manage these new types of risk, but sufficient techniques are not readily available.



# Key Requirements

High performers need advanced risk management techniques that enable them to

- assume an integrated view of risk (one view that includes process, technology, security, and interoperability risks)
- address the interrelated nature of risk (combinatorial effects and cascading consequences)
- understand the amount of risk that is inherited from partners and collaborators
- characterize the risk arising from the emergent properties of a distributed process

# What Is Risk?

The possibility of suffering harm or loss

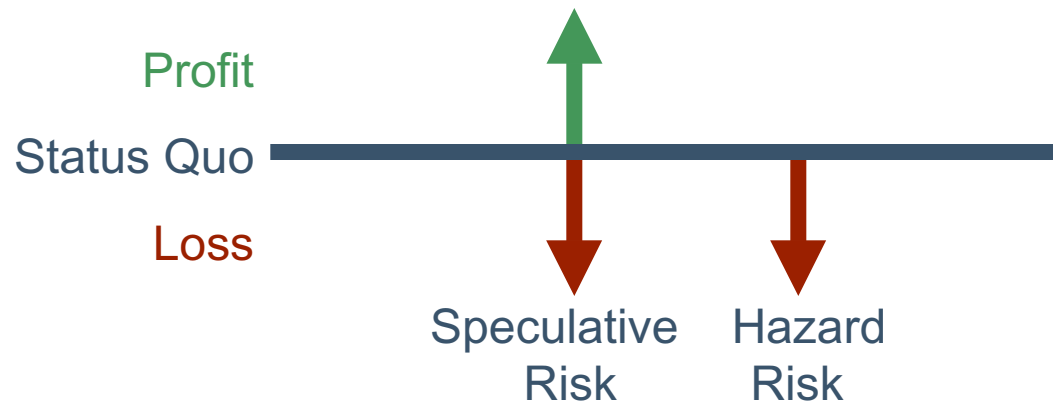
Risk requires the following conditions:

- loss
- uncertainty
- choice

# Nature of Risk

Speculative (dynamic) – a risk that has profit and loss associated with it

Hazard (static) – a risk that only has loss associated with it







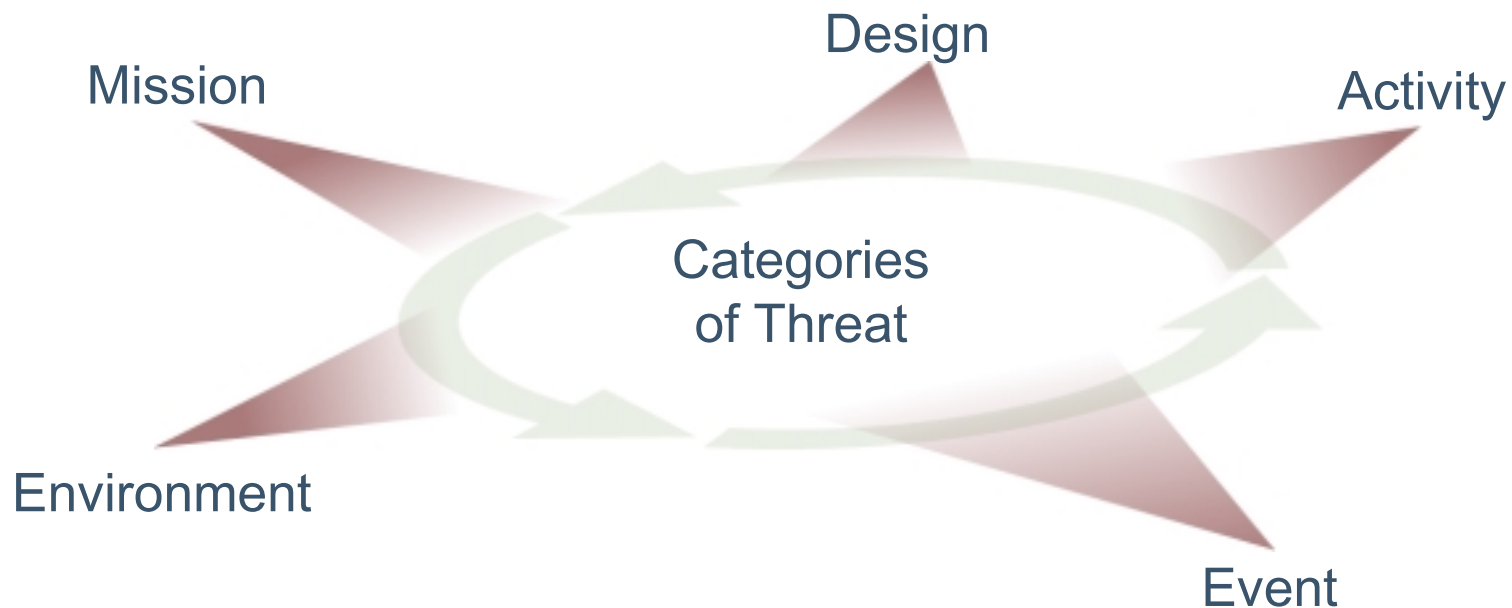
**Carnegie Mellon**  
**Software Engineering Institute**

# Operational Risk<sup>1</sup>

The risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events

1. Bank for International Settlements (BIS). *International Convergence of Capital Measurement and Capital Standards: A Revised Framework*. BIS, 2004. <http://www.bis.org/publ/bcbs107.pdf>.

## Sources of Risk During Operations



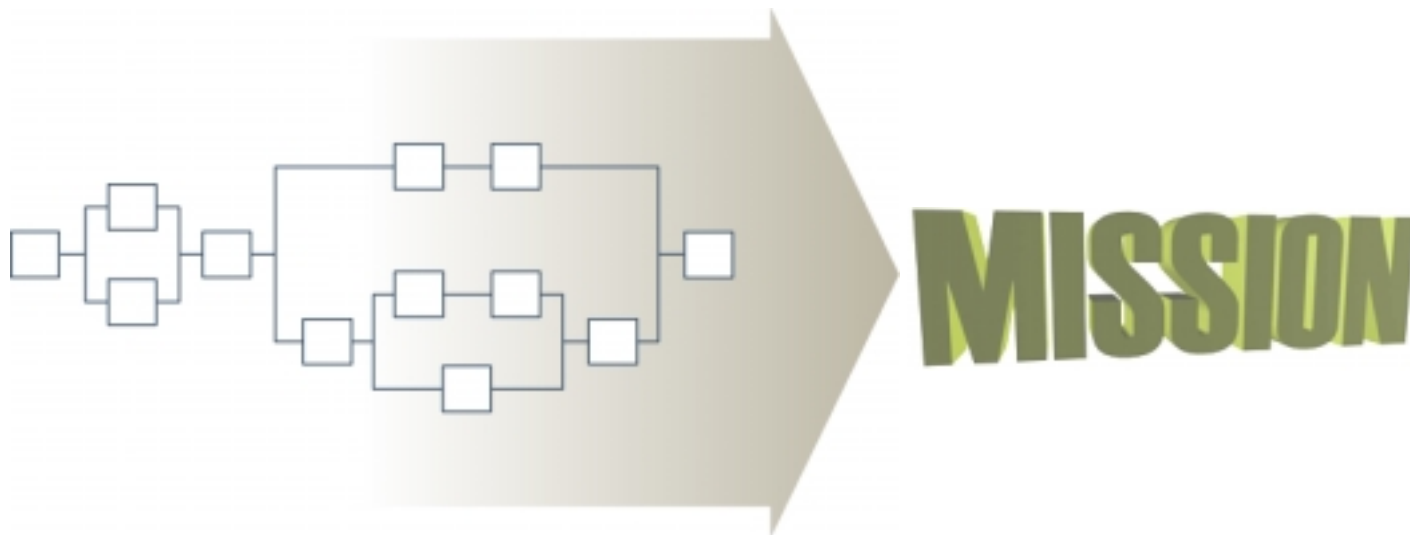
A broad range of threats must be considered when analyzing the potential for mission success.

# Mission

**MISSION**

A **mission threat** is a fundamental flaw, or weaknesses, in the purpose and scope of a work process.

# Process Design



A **design threat** is an inherent weakness in the layout of a work process.

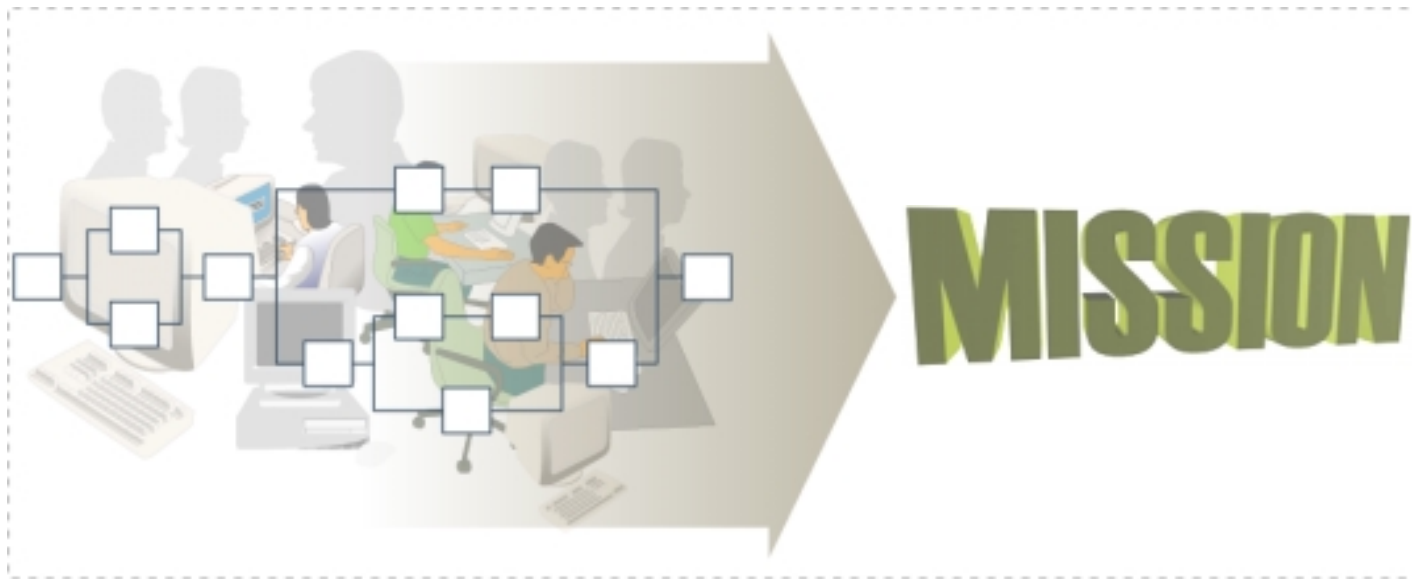
# Activity Management



An **activity threat** is a flaw, or weaknesses, arising from the manner in which activities are managed and performed.

# Operational Environment

Operational Environment



An **environment threat** is an inherent constraint, weakness, or flaw in the overarching operational environment in which a process is conducted.



# Event Management



An **event threat** is a set of circumstances triggered by an unpredictable occurrence that introduces unexpected change into a process.



**Carnegie Mellon**  
**Software Engineering Institute**

# Mission Risk

The possibility that a mission might not be successfully achieved





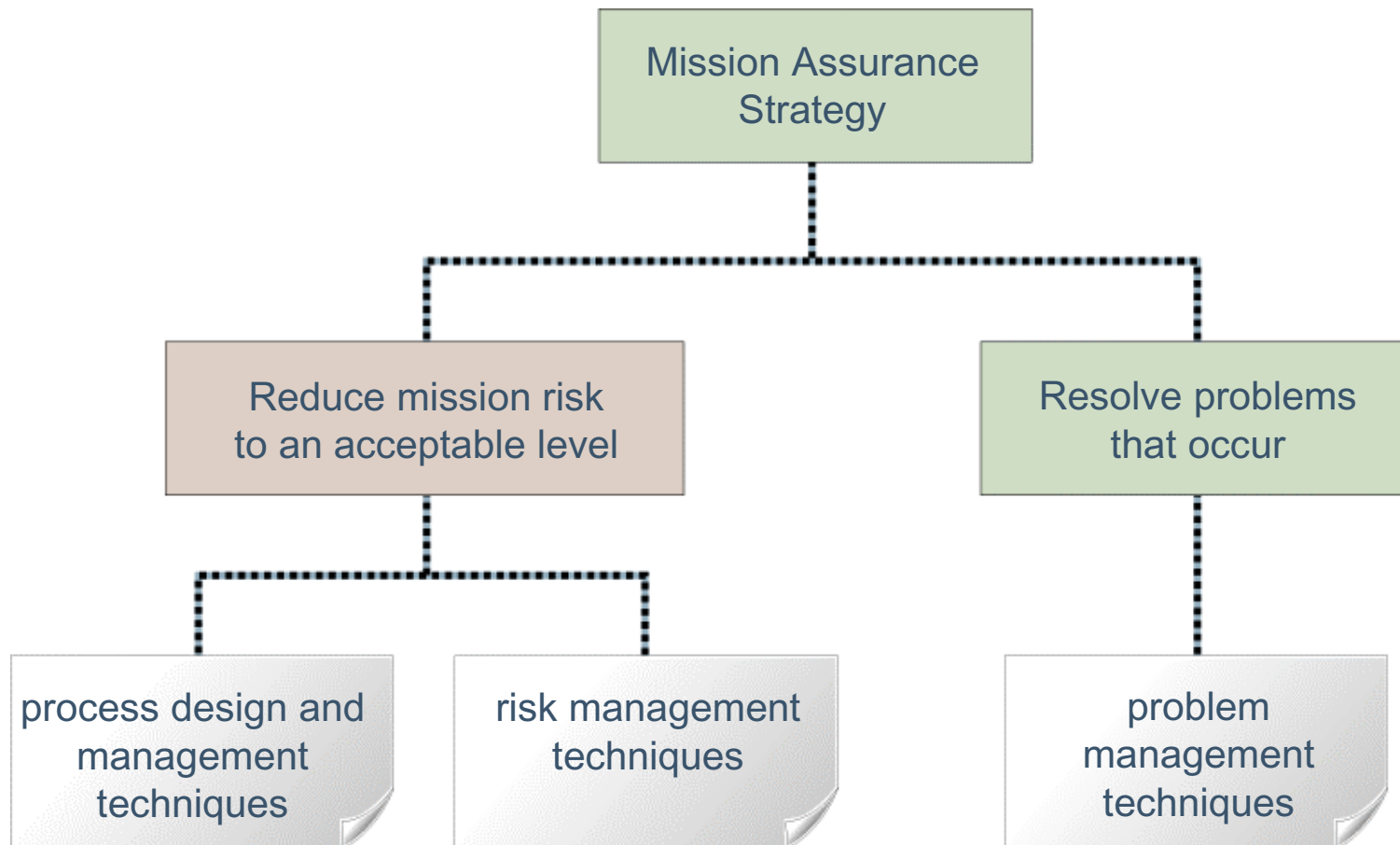
# Mission Assurance

Establishing a reasonable degree of confidence in mission success

Mission assurance is achieved by ensuring that risk to the mission (i.e., mission risk) is within tolerance.

A key aspect of mission assurance is its dual focus on outcome and execution.

# Mission Assurance Strategy





**Carnegie Mellon**  
**Software Engineering Institute**

## **What is MAAP?**

MAAP is a protocol, or heuristic, for determining the mission assurance of an operational process or system.



# Key Characteristics of MAAP

Applies an engineering approach to risk analysis

Designed for highly complex environments (multi-organization, system of systems)

Provides an in-depth analysis of processes, relationships, and dependencies

Characterizes the risk of mission failures

- process performance risk
- security risk
- operational environment risk



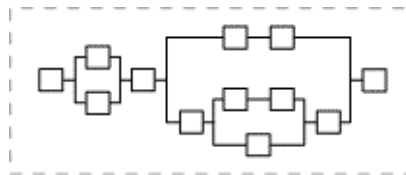
## **Structured Analysis of Performance**

MAAP analyzes process performance in multiple operational states

- normal, or expected, operational conditions
- unusual circumstances, or occurrences, triggered by external events

# Analyzing Multiple States

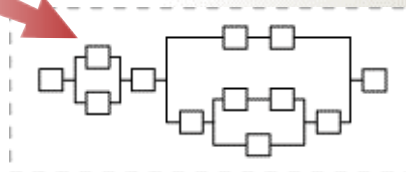
**State 1: Expected Operational Conditions**



*Risk during expected operational conditions*

**State 2: When Stressed by Event 1**

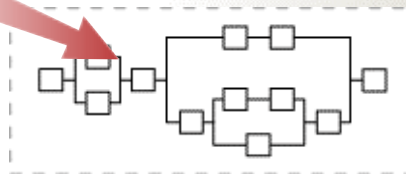
Event 1



*Risk resulting from event 1*

**State 3: When Stressed by Event 2**

Event 2

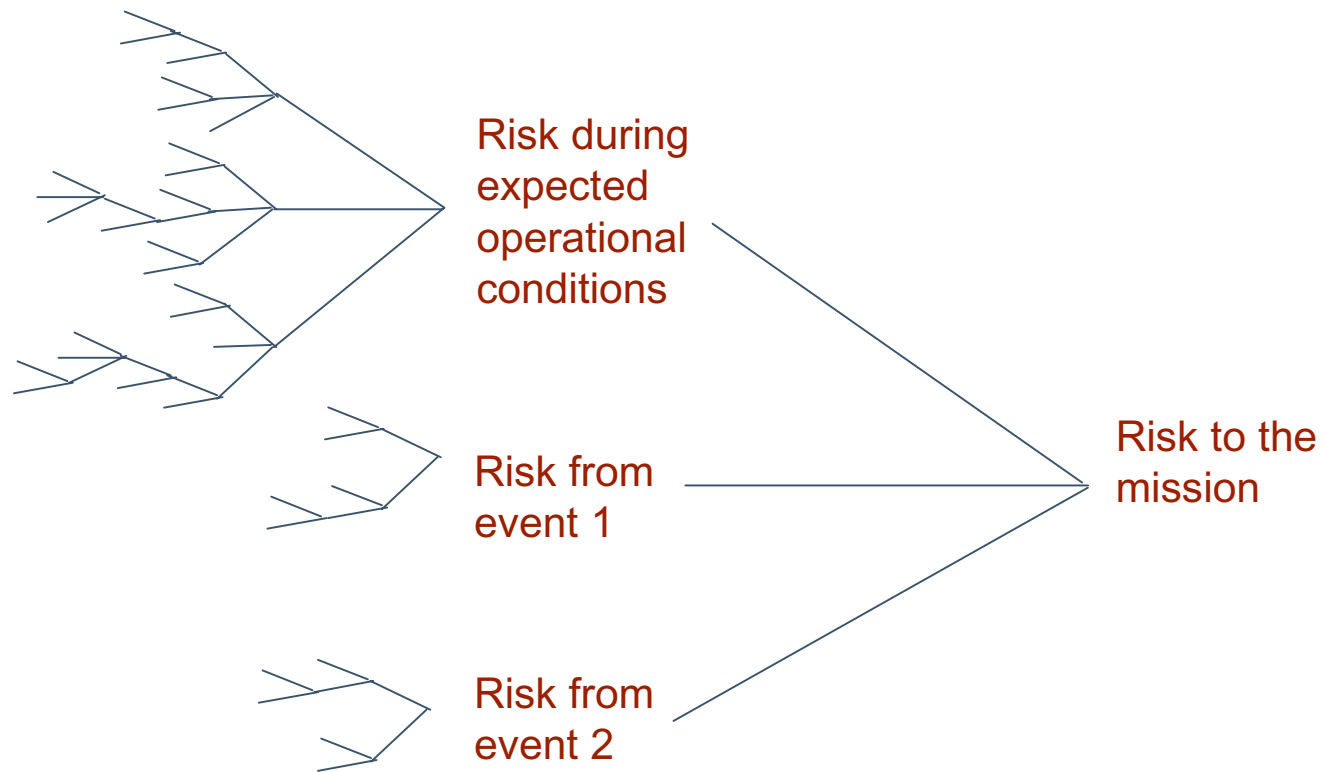


*Risk resulting from event 2*

**Risk to the mission**



# Risk Causal Chain



**Combinations of threats,  
vulnerabilities and controls**



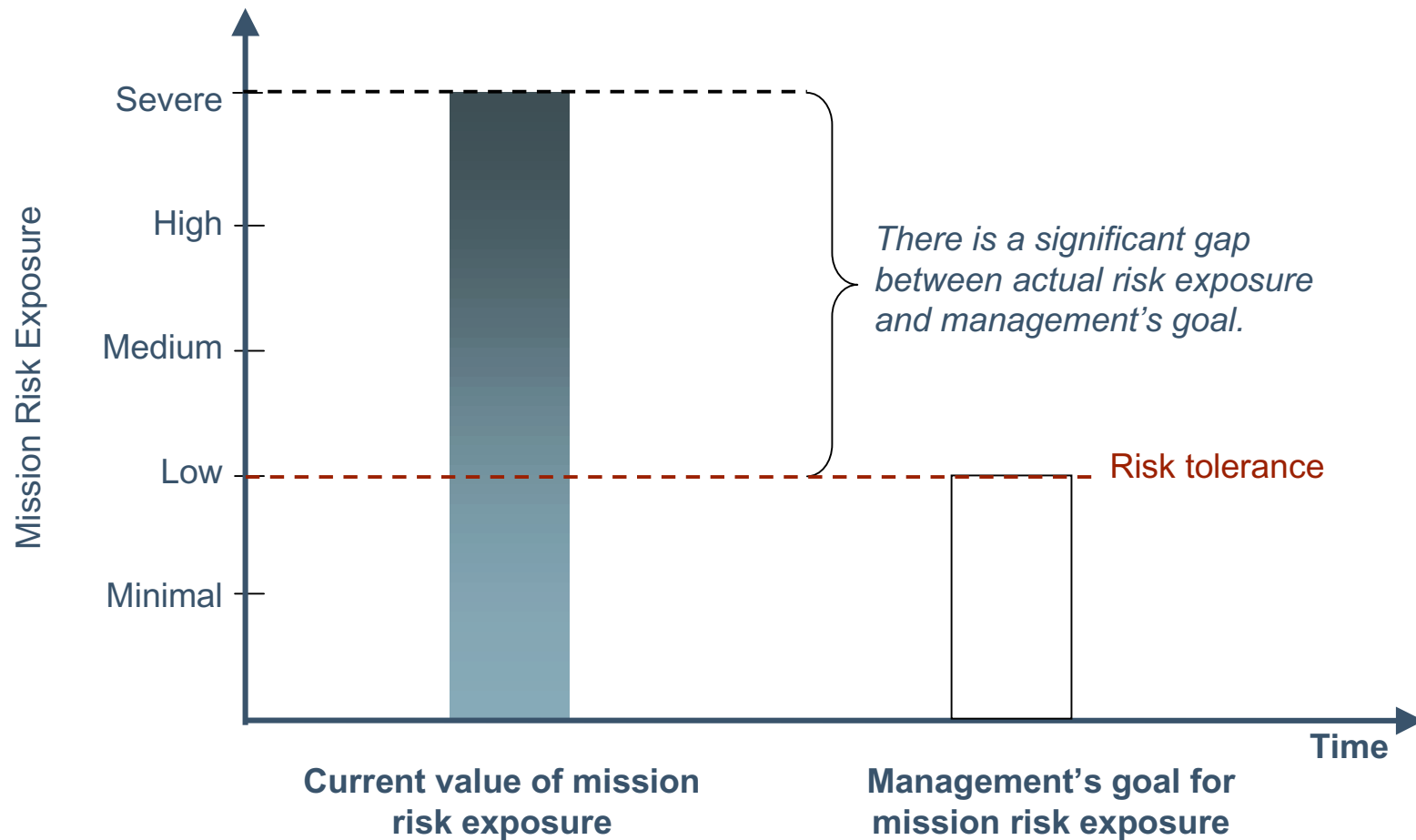
**Risk resulting from different  
operational circumstances**



**Mission risk**



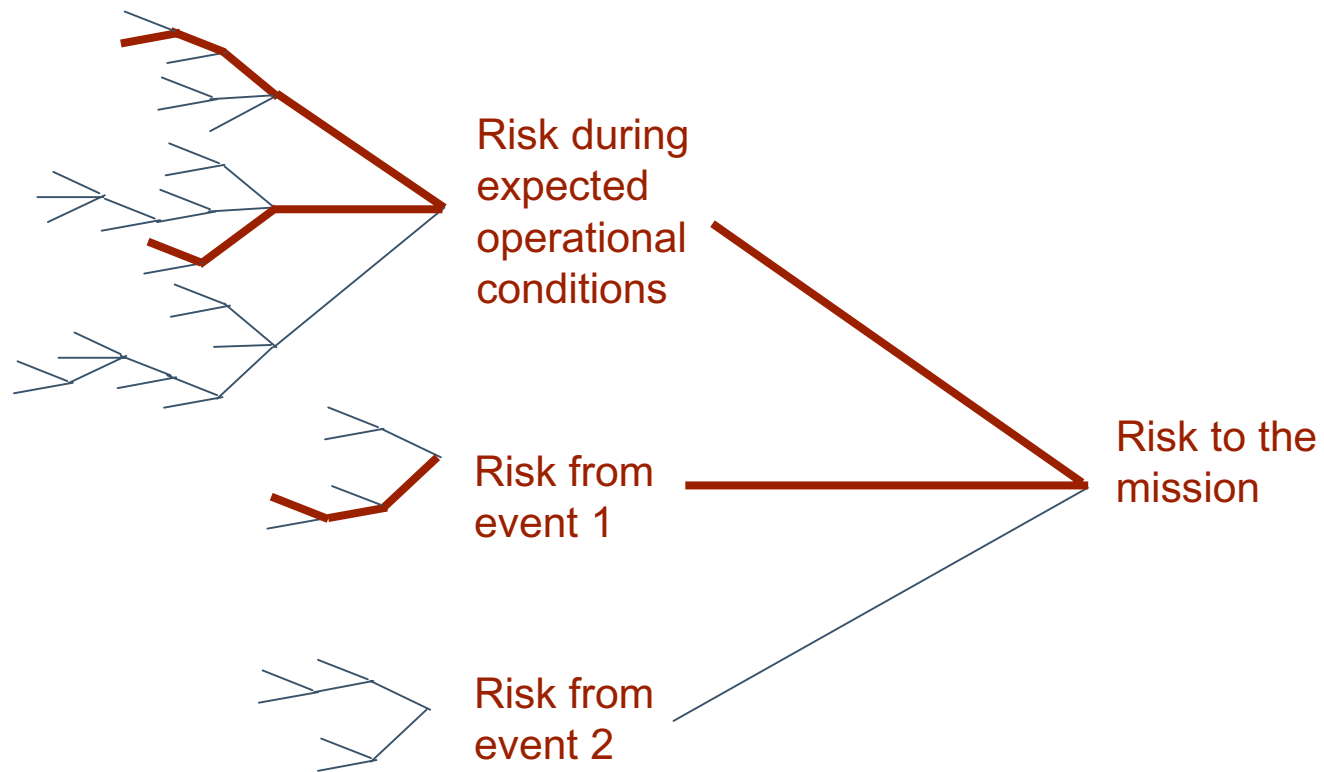
# Bringing Risk within Tolerance







# Key Risk Drivers



A critical path analysis identifies the key risk drivers.



# Protocol Fundamentals - 1

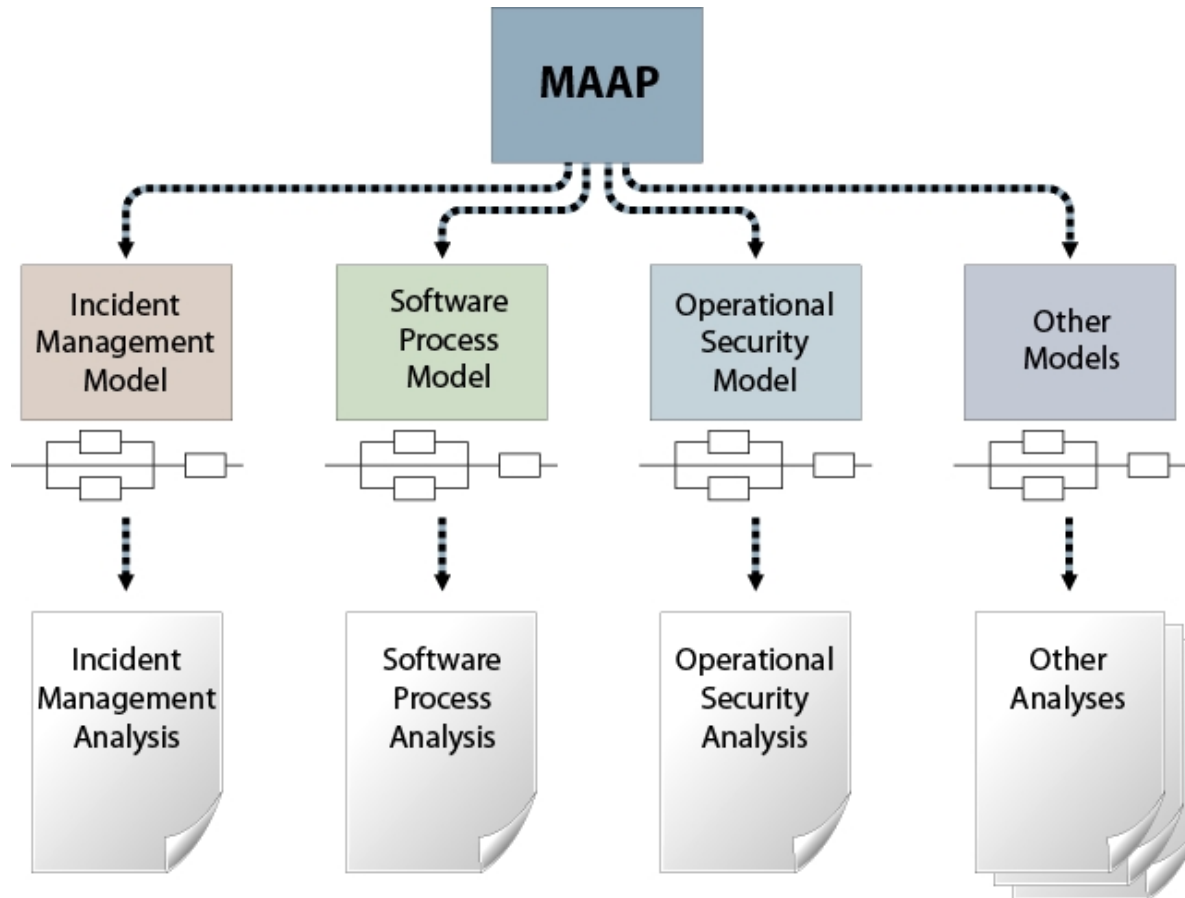
- Determine mission objectives.
- Characterize all operations conducted in pursuit of the mission.
- Define risk evaluation criteria in relation to the mission objectives.
- Identify potential failure modes.
- Perform a root cause analysis for each failure mode.



## **Protocol Fundamentals - 2**

- Develop a risk profile of the mission.
- Ensure that mission risk is within tolerance.

# A Common Basis for Analysis



## MAAP Pilot

Analyzed an incident management process in a large government organization

Analyzed risk to the mission under normal conditions

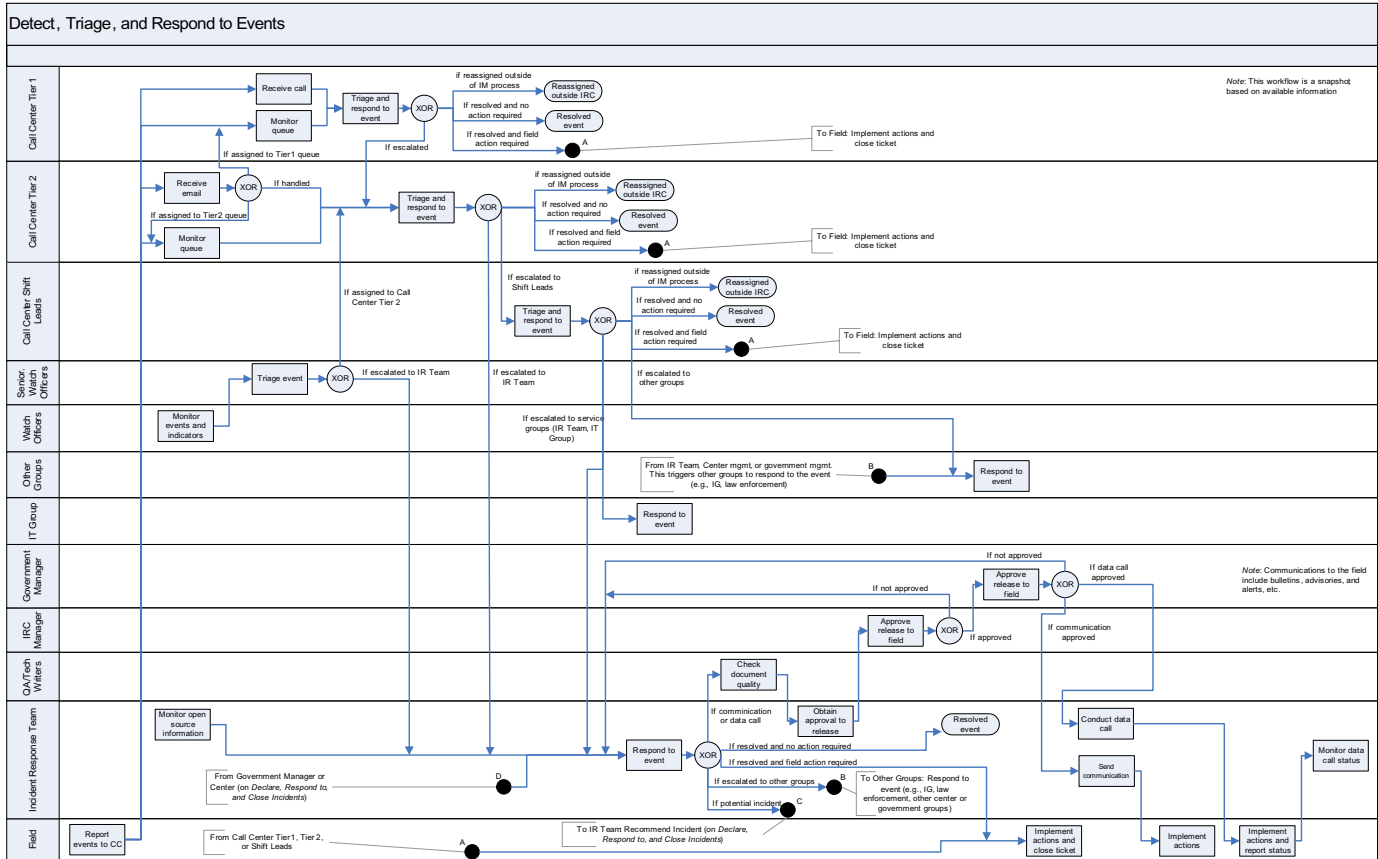
- quality of response
- timeliness of response
- customer satisfaction

Examined risk to the mission under unusual circumstances

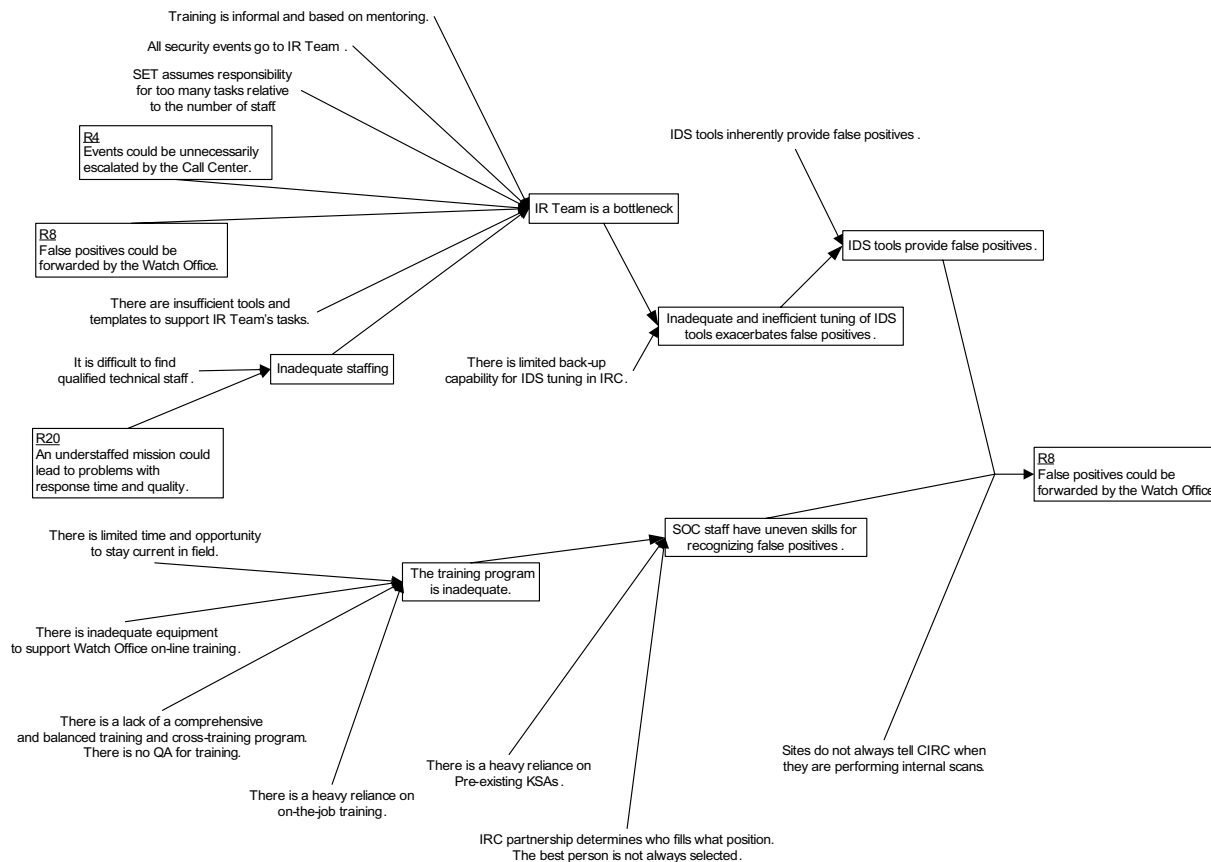
- two major incidents occur at the same time
- cyber security attack renders ticketing system unavailable for an extended period of time



## Example: Process Workflow

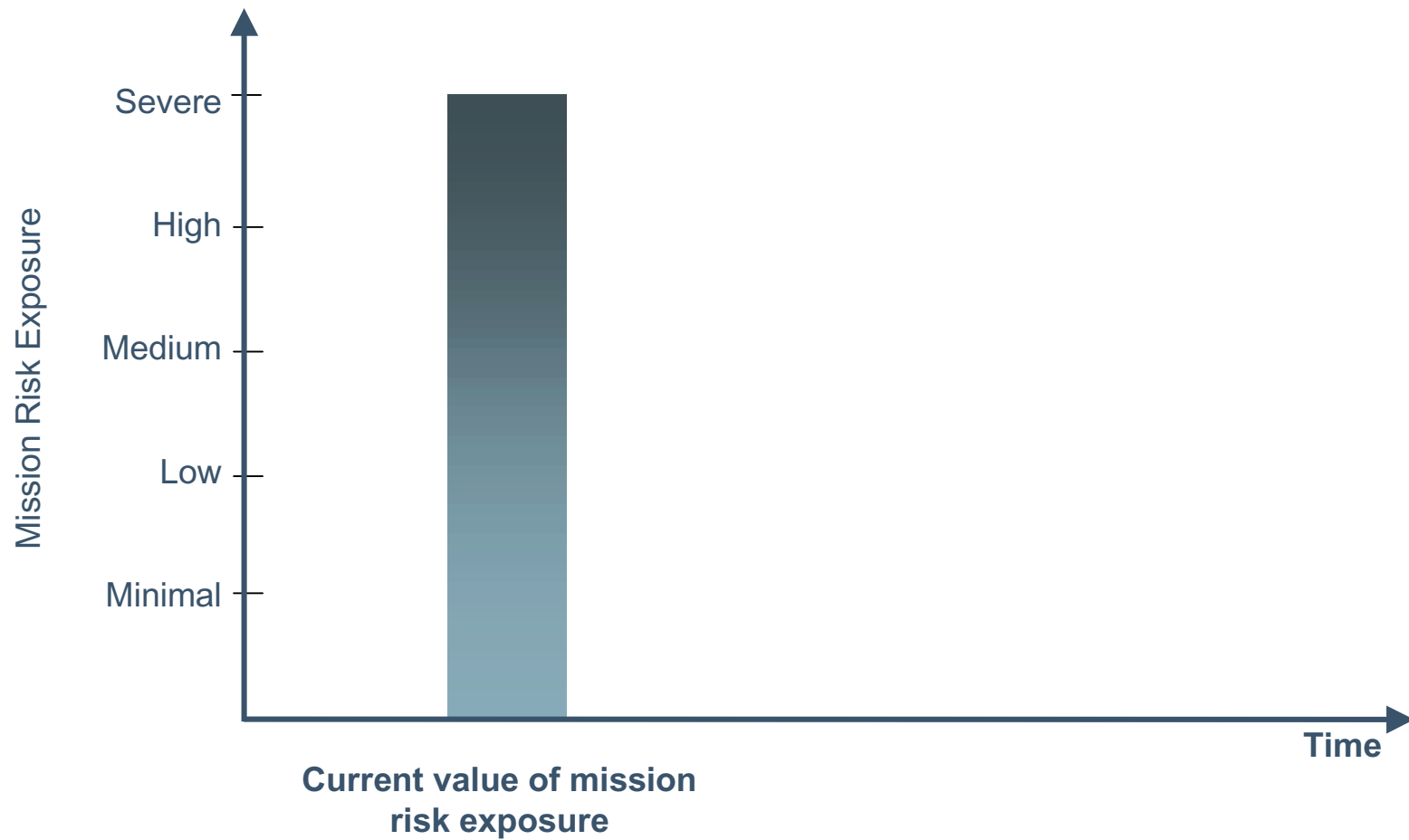


## Example: Complex Risks





## Example: Mission Risk







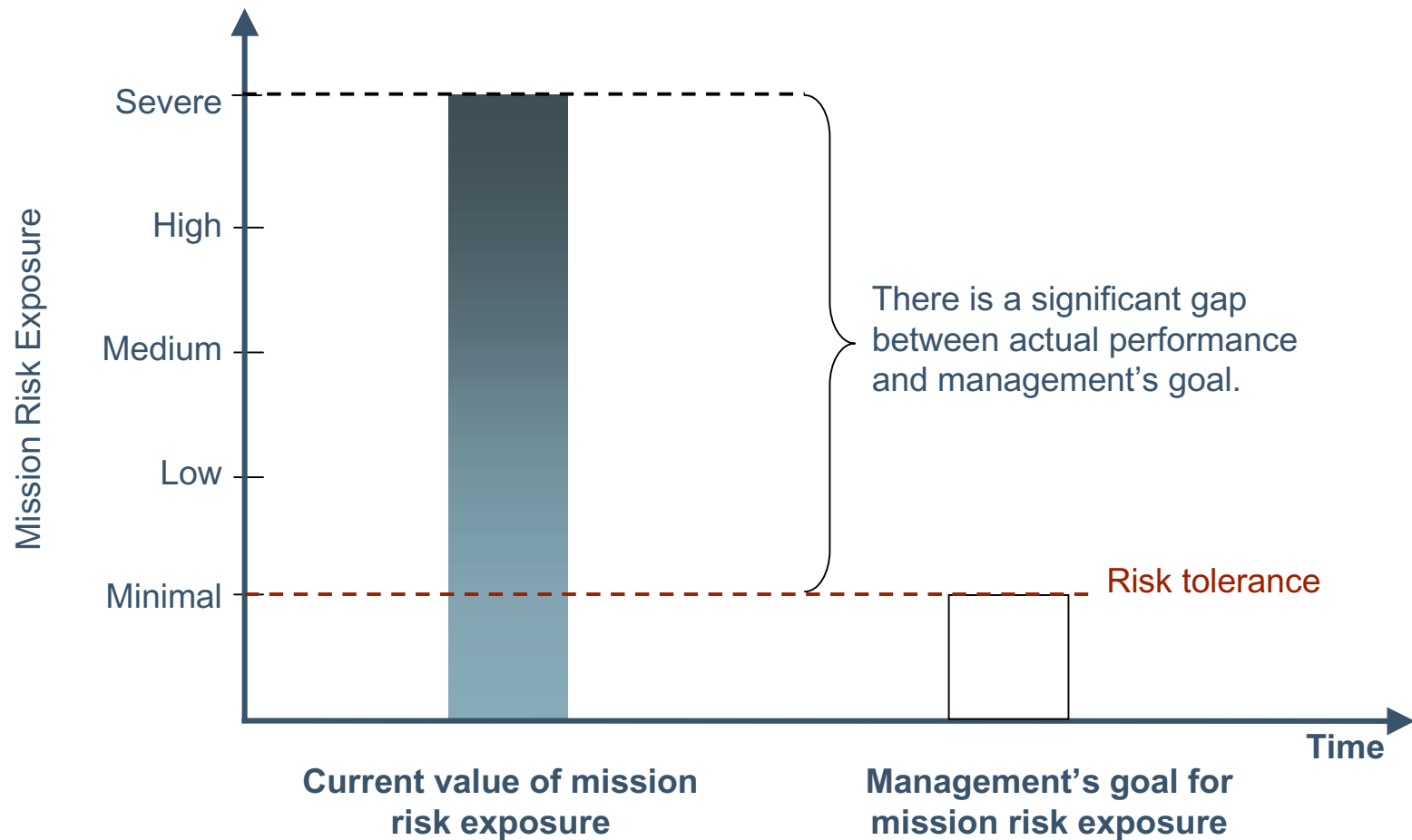
## **Example: Mission Assurance Goal**

Management's goal is to build a “world-class” incident management capability.

This goal translates to very high mission assurance (i.e., very low risk to the mission).



## Example: Gap in Performance





## **Example: Mitigation Strategy**

- Simplify the mission.
  - Determine which incident management services are essential.
  - Develop a plan for growing the incident management capability over time.
- Redesign the process based on the revised mission.
- Develop and test contingency plans.



## Conclusions

Many types of risk prevalent in today's operational environments (e.g., event risks, inherited risk) are not readily identified using traditional risk analysis techniques.

High-performing organizations have the basic skills needed to identify and manage these new types of risk, but lack sufficient techniques.

Average or poor performers will not have the skills needed to identify and manage new types of risk (and probably have bigger, more obvious risks to deal with).

MAAP is one technique that high performers can use to identify and mitigate the risks arising from operational complexity.



## **Additional Research and Development**

Develop a technique for quickly estimating mission risk exposure.

- First pilot will focus on mission assurance in incident management.
- Second pilot will focus on mission assurance in system development.

Refine and document MAAP based on pilot experience.

Pilot MAAP in another domain.



**Carnegie Mellon**  
**Software Engineering Institute**

## Contact Information

Telephone      412 / 268-5800

Fax              412 / 268-5758

WWW            [http://www.sei.cmu.edu/programs/  
acquisition-support/](http://www.sei.cmu.edu/programs/acquisition-support/)

U.S. mail        Customer Relations  
                     Software Engineering Institute  
                     Carnegie Mellon University  
                     Pittsburgh, PA 15213-3890